

Before the
Federal Communications Commission
Washington, D.C. 20554

In re Petition for Rulemaking) Proceeding RM-11699
Don Rolph) Encryption of Amateur Radio Communications
Petitioner) COMMENT
Filed June 7, 2013)
)
)
)
)

I support a change in the Amateur Radio Service rules to permit encoding of messages to obscure meaning in the case of communications emergencies, communications in support of emergency operations or disaster-relief operations, and bona fide practice and training.

This change would be in the public interest by permitting amateur operators to provide communications of content which should not be divulged to the public. This change would be consistent with the provisions of 47 CFR § 97.403, which provides that “[N]o provision of these rules prevents the use by an amateur station of any means of radiocommunication at its disposal to provide essential communication needs in connection with the immediate safety of human life and immediate protection of property when normal communication systems are not available.” This change would also be consistent with one of fundamental purposes for the establishment of the Amateur Radio Service at 47 CFR § 97.1(a), i.e., providing emergency communications.

Although there are some amateur operators who fear that this change in the rules would somehow encourage amateurs to transmit encrypted communications in situations not authorized by the

Commission's rules, I have seen no evidence that this change would somehow motivate licensed amateurs to violate the rules.

I. RULE CHANGE WILL BENEFIT THE PUBLIC

It is easy to list scenarios where the public would best be service by encrypting communications, and here are some examples.

Medical treatment. The unavailability of conventional communications channels to support communications in support of a medical emergency can occur in conjunction with a natural or man-made disaster (e.g., hurricane, or a remote plane crash), or simply as a result of a technical problem (severed fiber optic cable). In many cases – e.g., ordering supplies or alerting emergency room staff – there would be no need to communicate personal information about a patient. But in some cases – e.g., if it would be helpful for a first responder to have access to patient records from a hospital or physician – it would be necessary to identify the patient in order to retrieve the needed records. The public interest – as well as compliance with HIPAA – would be best served if this information were not carried on a channel which could be intercepted by others.

Financial information. Part of disaster relief is procuring disaster-relief goods and services from vendors, and in general these vendors expect to be paid. The universal method of payment is bank cards, but bank card information should not be transmitted over an open radio channel because of the risk of identify theft and fraud. The public interest would be best served if bank card information could be provided to a vendor in payment for vital disaster-relief goods and services without the risk of interception of this sensitive information.

Law enforcement. Looting and violent crime are not unusual in disaster situations, and in some cases law enforcement personnel may need to coordinate a response. If this kind of tactical information is passed on an open radio channel, it could find its way directly or indirectly to the perpetrators and

frustrate the law enforcement response. The public interest would be best served if law enforcement communications could be encrypted when deemed necessary by law enforcement agencies.

Coordination of transportation and distribution efforts. As part of disaster response or in other emergency situations, it is often necessary to coordinate the transportation of resources such as drugs and food. In order to help mitigate the risk of robbery or theft of the transported goods, it can sometimes be best for the transportation arrangements to not be made available to the public. The public interest would be best served if communications for the coordination of the transportation of certain emergency goods could be conducted over a secure channel.

II. RULE CHANGE WILL NOT HARM THE PUBLIC

Some may be concerned that the public will be harmed if encrypted communications are permitted under additional limited circumstances in the Amateur Radio Service, as radio operators would somehow be motivated to transmit encrypted communications of prohibited content.

However, this fear is unfounded. Encrypted communications in limited circumstances have been permitted by the rules for years (e.g., telecommand messages to control a space station), and yet a search of Enforcement Bureau documents does not show even one instance where the Commission has even warned an amateur operator about transmitting an encoded message.

Others may be concerned that with an exception for emergencies and drills, it will be impossible to determine whether the content of an encoded transmission is in fact permitted by the rules; however, this concern is also unfounded. It is not difficult to determine whether an emergency is in fact in progress, as the kind of emergency for which amateur radio communication support is appropriate would usually be a well-publicized natural or man-made disaster. Training exercises would also be easily recognizable on the air. Any communications in violation of the rules would require a conspiracy of at least two station operators – at the transmitting and receiving ends. Amateur operators have a long history and tradition of complying with Commission rules, and a conspiracy between two (or more) operators is not likely.

1 If Commission monitoring staff were to monitor a suspicious transmission, there is no obstacle to
2 the Commission contacting the station licensees and asking for clarification of the circumstances. And if
3 a member of the public overhears a suspicious encoded transmission – e.g., if a concerned licensed
4 amateur operator hears an encrypted message when it appears no emergency or training exercise in
5 progress – there is nothing which would stop that operator from communicating his concerns to the
6 Commission for such investigation as the Commission deems appropriate.

7 Furthermore, it is hard to even identify a potential motivation for operators to use encoded
8 messages on amateur bands. The Commission rules provide spectrum allocations for government and
9 business communications, and there is no prohibition against encrypted messages in those services. For
10 short-range communications, there is no prohibition in the rules against obscuring the meaning of FRS
11 and MURS voice communications – and neither service even requires a license. And data transmissions
12 – including transmissions with obscured meaning – are permitted on MURS channels. It is hard to
13 imagine why anybody would not simply obtain the necessary license and equipment if there is a need for
14 routine encrypted communications. Without any apparent motivation to use Amateur Radio Service
15 spectrum for encrypted prohibited content, it is hard to imagine that this would occur.

16 Finally, even if there were rare isolated instances of encrypted prohibited content transmitted on
17 Amateur bands, there would be no material harm to the public. No specific frequency is dedicated to any
18 particular amateur station or operator, and amateur operators are skilled in finding a suitable alternate
19 suitable channel for communications in the event that a channel is in use or unusable for any reason.

21 III. RECOMMENDATION

22 I recommend that the Commission modify the Amateur Radio Service rules to permit, in the case
23 of emergencies, encoded messages intended to obscure meaning.

24 If the Commission is not prepared to take immediate action to change the rules, I believe the
25 publishing by the Commission of a Notice of Inquiry may be appropriate, where the Commission

1 specifically seeks feedback from government and non-government emergency managers about the
2 benefits of having the option, in emergencies, to use Amateur Radio Service operators and spectrum to
3 send messages with obscured meaning. This would also be an opportunity for those who are concerned
4 about abuse (from the transmission of encoded prohibited content) to submit evidence quantifying the
5 likelihood of such abuse, the expected frequency of such abuse, and how any harm to the public from a
6 rule change will exceed the expected benefit of the change. (But I expect that it will be difficult for
7 opponents to come up with any objective evidence about how the proposed rule change will harm the
8 public.)

9 I also recommend that in the event the Commission does not deem it appropriate to promptly
10 update the rules as requested by the Petitioner, the Commission issues a short-term waiver to
11 accommodate encrypted emergency communications while rulemaking proceedings are pending.

12 Dated this 7th day of July, 2013.

13 Respectfully,

14
15 /signature/

16 David A. Behar
17 P.O. Box 40204
18 Spokane, WA 99220

19 Petitioner Don Rolph has agreed to be served via electronic mail, and this filing has been served
20 on him via electronic mail before it was filed via ECFS.

21 /signature/

22 David A. Behar
23 P.O. Box 40204
24 Spokane, WA 99220
25